ICS 25.040
N 10

中华人民共和国国家标准化指导性技术文件

GB/Z 29638—2013/IEC/TR 61508-0:2005

电气/电子/可编程电子安全相关系统的功能安全　功能安全概念及GB/T 20438系列概况

Functional safety of electrical/electronic/ programmable electronic safety-related systems—Functional safety and GB/T 20438

(IEC/TR 61508-0:2005,IDT)

2013-07-19 发布　　2013-12-15 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　次

前　言

GB/T 20438《电气/电子/可编程电子安全相关系统的功能安全》由下列7个部分构成：

——第1部分：一般要求；

——第2部分：电气/电子/可编程电子安全相关系统的要求；

——第3部分：软件要求；

——第4部分：定义和缩略语；

——第5部分：确定安全完整性等级的方法示例；

——第6部分：GB/T 20438.2和GB/T 20438.3的应用指南；

——第7部分：技术和措施概述。

本指导性技术文件，是对GB/T 20438标准的补充。它主要介绍功能安全的概念以及GB/T 20438系列标准的概况，本指导性技术文件可与GB/T 20438系列标准配套使用。

本指导性技术文件按照GB/T 1.1—2009给出的规则起草。

与本文件中规范性引用的国际文件有一致性对应关系的我国文件如下：

——GB/T 16499—2008　安全出版物的编写及基本安全出版物和多专业共用安全出版物的应用导则(IEC Guide 104:1997,NEQ)

——GB/T 20000.4—2003　标准化工作指南　第4部分：标准中涉及安全的内容(ISO/IEC Guide 51:1999,MOD)

本指导性技术文件等同采用IEC/TR 61508-0:2005《电气/电子/可编程电子安全相关系统的功能安全　第0部分：功能安全概念及IEC 61508系列概况》。

本指导性技术文件的技术内容与IEC/TR 61508-0:2005等同，为了便于使用，做了如下编辑性修改：

——删除国际标准的前言，按GB/T 1.1—2009重新编写了本文件的前言；

——正文中，凡是出现“IEC 61508”之处均改为“GB/T 20438”；

——凡是出现“本技术报告”之处均改为“本文件”；

——根据GB/T 1.1—2009进行格式编辑性修改。

本指导性技术文件由中国机械工业联合会提出。

本指导性技术文件由全国工业过程测量和控制标准化技术委员会(SAC/TC 124)归口。

本指导性技术文件主要起草单位：机械工业仪器仪表综合技术经济研究所、上海自动化仪表股份有限公司、上海工业自动化仪表研究院、北京和利时系统工程有限公司、深圳市步科电气有限公司、北京市劳动保护科学研究所、斯堪伯奥科技(北京)有限公司、菲尼克斯电气(南京)研发工程中心有限公司、中国铁道科学研究院、中机生产力促进中心、浙江大学智能系统与控制研究所、皮尔磁工业自动化贸易(上海)有限公司、华中科技大学控制系、西门子(中国)有限公司。

本指导性技术文件主要起草人：丁露、王春喜、欧阳劲松、史学玲、孟邹清、包伟华、李佳嘉、罗安、池家武、靳江红、王海清、张龙、张萍、张晓飞、冯冬芹、褚卫中、周纯杰、李佳。

引　言

本指导性技术文件的目的是介绍功能安全的概念，并提供 GB/T 20438 系列标准的概述。

当您有如下需求时可阅读本指导性技术文件：

——判断 GB/T 20438 是否适用于您；

——参与可能涉及安全的电气/电子/可编程电子系统的开发；

——起草功能安全相关的任何其他标准。

本指导性技术文件的第 3 章给出功能安全的非正式定义，描述了安全功能、安全完整性和安全相关系统之间的关系、给出如何得出功能安全要求的示例，并列出了一些用电气/电子/可编程电子系统实现功能安全将遇到的挑战。第 4 章介绍了 GB/T 20438 的具体内容，提供了实现功能安全的方法，并描述了 GB/T 20438 的目的、技术方法和框架。它阐述了 GB/T 20438 可广泛地用于不同行业，并可作为许多其他标准的基础。

电气/电子/可编程电子安全相关系统的功能安全　功能安全概念及GB/T 20438系列概况

1　范围

本指导性技术文件介绍了功能安全的概念及GB/T 20438系列的概况。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GB/T 20438.1—2006　电气/电子/可编程电子安全相关系统的功能安全　第1部分：一般要求(IEC 61508-1:1998,IDT)

GB/T 20438.2—2006　电气/电子/可编程电子安全相关系统的功能安全　第2部分：电气/电子/可编程电子安全相关系统的要求(IEC 61508-2:2000,IDT)

GB/T 20438.3—2006　电气/电子/可编程电子安全相关系统的功能安全　第3部分：软件要求(IEC 61508-3:1998,IDT)

GB/T 20438.4—2006　电气/电子/可编程电子安全相关系统的功能安全　第4部分：定义和缩略语(IEC 61508-4:1998,IDT)

GB/T 20438.5—2006　电气/电子/可编程电子安全相关系统的功能安全　第5部分：确定安全完整性等级的方法示例(IEC 61508-5:1998,IDT)

GB/T 20438.6—2006　电气/电子/可编程电子安全相关系统的功能安全　第6部分：GB/T 20438.2和GB/T 20438.3的应用指南(IEC 61508-6:2000,IDT)

GB/T 20438.7—2006　电气/电子/可编程电子安全相关系统的功能安全　第7部分：技术和措施概述(IEC 61508-7:2000,IDT)

IEC Guide 104　安全出版物的编写及基本安全出版物和多专业共用安全出版物的应用导则(The preparation of safety publications and the use of basic safety publications and group safety publications)

ISO/IEC Guide 51　安全方面　在标准中引入安全条款的指南(Safety aspects—Guidelines for their inclusion in standards)

3　功能安全

3.1　功能安全是什么

安全是指避免会造成人体健康损害或人身损伤的不可接受风险，而这种风险是由于对财产或环境的破坏而直接或间接地导致的。

功能安全是整体安全的一部分，它依赖于一个系统或设备对其输入的正确响应。

例如，在电机绕组上装一个热传感器，可以在电机过热前实现断电的过热保护装置是功能安全的一个例子。但用特殊的隔热材料来抵御高温就不是功能安全的例子(虽然这也是实现安全的一个例子，并

能抵御同样的危险)。

安全或功能安全的确定需将各个系统视为一个整体,并且考虑各系统所处的交互环境。

3.2 安全功能及安全相关系统

一般来说,设备及相关的所有控制系统在特定环境下的重大危险必须由专业人员或开发人员通过危险分析来识别。该分析确定是否需要通过功能安全对每个重大危险提供足够的保护。如果需要,则应考虑在设计中采取适当方法实现。功能安全只是应对危险的方法之一,同时其他消除或降低危险的方法,如通过设计实现固有安全,是至关重要的。

术语"安全相关"用来描述这样的系统,该系统执行一个或多个特定功能以确保将风险保持在一个可接受的水平。根据定义,这样的功能就是安全功能。为实现功能安全,下面两种要求是必要的:

——安全功能要求(功能用来做什么);

——安全完整性要求(安全功能按要求执行的可能性)。

安全功能要求由危险分析确定,安全完整性要求由风险评估确定。安全完整性的等级越高,危险失效发生的可能性越低。

无论采用什么技术执行安全功能的系统,就是安全相关系统。安全相关系统可独立于设备控制系统,或者设备控制系统本身可实现安全功能。后者中,设备控制系统就是一个安全相关系统。安全完整性的等级越高,安全相关系统的工程实施要求越严格。

3.3 功能安全示例

设想一台机器,其旋转叶片由铰接硬质防护罩来保护。需要打开防护罩进行例行清洁时,可能触及叶片。防护罩是联锁的,在防护罩打开时电机断电、启动刹车,使叶片在可能伤害到操作员前停止旋转。

为了保证安全,有必要进行危险分析和风险评估。

a) 通过危险分析识别清洁叶片可能出现的危险。对此机器,在启动刹车并使叶片停止前,铰接防护罩的开度不能超过 5 mm。进一步分析显示,使叶片停止的时间不应超过 1 s。以上这些描述了安全功能的要求。

b) 通过风险评估确定安全功能的性能要求。其目的是保证安全功能的安全完整性足够保证危险事件不会使人处于不可接受的风险环境中。

安全功能失效导致的伤害可能是操作人员的手被切断或仅仅是擦伤。风险还取决于防护罩打开的频率,可能是一天多次或少于一月一次。所要求的安全完整性等级随着伤害的严重程度和暴露于危险环境频率的增加而提高。

安全功能的安全完整性取决于正确执行安全功能所需的所有设备,即联锁、相关电路、电机和刹车系统等。安全功能及其安全完整性规定了在特定环境下各系统作为一个整体所要求的行为。

总之,危险分析识别如何避免与叶片相关的危险事件发生。风险评估给出为使风险可接受的联锁系统所要求的安全完整性。如下两个因素:"哪些安全功能必须执行"即安全功能要求,和"执行安全功能所必需的确定性程度如何"即安全完整性要求,是功能安全的基础。总之,危险分析识别如何避免与叶片相关的危险事件发生。

3.4 实现功能安全的挑战

安全功能越来越多地由电气、电子或可编程电子系统执行。这些系统通常很复杂,不可能在实际中完全确定其每种失效模式或测试所有可能的行为。尽管测试是必要的,但很难预测其安全性能。

防止危险失效或出现危险失效时对其进行控制,是系统设计时面对的挑战。危险失效来自:

——错误的系统、硬件或软件规范;

——安全要求规范的遗漏(例如,未明确在不同操作模式下所有相关安全功能);

——随机硬件失效机制；
——系统硬件失效机制；
——软件错误；
——共因失效；
——人因错误；
——环境影响(例如电磁、温度、机械因素)；
——供电系统的电压扰动(例如断电、欠压、供电恢复)。
GB/T 20438 包括最大限度地减少这些失效的要求，详见第 4 章。

4 GB/T 20438 E/E/PE 安全相关系统的功能安全

4.1 目的

GB/T 20438 的目的是：
——发挥 E/E/PE 技术的潜在优势，提高安全性和经济性；
——在整体安全的框架内推动技术的发展；
——提供技术上完整的、基于系统的方法，为未来提供充分的灵活性；
——提供基于风险的方法，确定安全相关系统的性能要求；
——提供可以在工业中直接使用的通用标准，也可用来帮助制定各领域标准(例如机械、化工、医疗或铁路)或产品标准(例如动力驱动系统)；
——在使用基于计算机的技术时，为用户和管理当局提供一种增强信心的手段；
——提供基于共同基本原则的要求，以促进：
- 为不同领域的子系统和器件的供应商提高供应链效率；
- 改善交流和要求(更清晰地描述需要规定的内容)；
- 开发可跨领域使用的技术和措施，增加可用的资源；
- 需要的情况下，开发一致性评估服务。

GB/T 20438 不包括那些可能是必要的预防措施，这些措施用以防止未授权的人员对 E/E/PE 安全相关系统实现功能安全的破坏，和/或其他负面影响。

4.2 E/E/PE 安全相关系统

GB/T 20438 针对安全相关系统实现的功能安全，而这些系统主要采用电气/电子/可编程电子(E/E/PE)技术，即 E/E/PE 安全相关系统。GB/T 20438 适用于这些系统，而不考虑其应用。

GB/T 20438 的一些要求与开发活动相关，其中的实现技术可能尚未完全确定。这包括整体安全要求的开发(概念、范围定义、危险分析和风险评估)。如果可能用到 E/E/PE 技术，则应使用 GB/T 20438以一种系统的、基于风险的方式来确定所有 E/E/PE 安全相关系统的功能安全要求。

GB/T 20438 的其他要求，包括文档、功能安全管理、功能安全评估和资质，并非专用于 E/E/PE 技术。非技术特定的所有要求也可有效地应用于其他安全相关系统，但这些系统不在 GB/T 20438 的范围内。

下面是 E/E/PE 安全相关系统的示例：
——危险化工厂的紧急停车系统；
——起重机安全负载指示器；
——铁路信号系统；
——机械联锁防护和紧急停机系统；
——变速电机限速保护装置；

——医用放射性设备的辐射剂量联锁系统和控制系统；
——动态定位(接近海上平台时的船舶运动控制)；
——飞行器控制面的线控操作；
——汽车指示灯、防抱死刹车和发动机管理系统；
——通过网络对处理装置进行远程监视、操作或编程；
——错误结果会影响安全的信息决策支持工具。

一个 E/E/PE 安全相关系统涵盖执行安全功能所需的所有系统部件(即从传感器开始，通过控制逻辑和通信系统，到最终执行器，包括操作员的任何关键动作)。

由于 E/E/PE 安全相关系统的定义来自于安全的定义，所以它也涉及避免对人体健康造成损伤和伤害的不可接受的风险。伤害可能间接的来自财产或环境的破坏。但是，一些系统主要设计用于防止导致严重经济损失的失效。GB/T 20438 可用于开发具有关键功能的 E/E/PE 系统，比如对设备或产品的保护。

4.3 技术方法

GB/T 20438
——采用基于风险的方法来确定 E/E/PE 安全相关系统的安全完整性要求，还包括大量的应用示例；
——对于确保 E/E/PE 安全相关系统实现功能安全所必要的活动，采用整体安全生命周期模型作为这些活动的技术框架；
——涵盖所有的安全生命周期活动，从初始概念、到危险分析和风险评估、制定安全要求、规范、设计和实现、操作与维护、改进，直到最后的停用和/或处置；
——涵盖系统(系统由执行安全功能的所有子系统构成，包括硬件和软件)和失效机制(随机硬件和系统)；
——包括防止失效的要求(避免故障的引入)和控制失效的要求(保证故障出现时的安全)；
——规定了达到要求的安全完整性所需的技术和措施。

4.4 安全完整性等级

GB/T 20438 将安全功能的安全性能划分了 4 个等级，即安全完整性等级。SIL1 是最低的等级，SIL4 是最高的等级。GB/T 20438 详细说明了实现每个安全完整性等级的要求。安全完整性等级越高，要求越严格，以达到所要求的更低的危险失效可能性。

一个 E/E/PE 安全相关系统通常执行多个安全功能。如果各安全功能的安全完整性要求不同，除非各安全功能的实现有充足的独立性，否则整个 E/E/PE 安全相关系统应采用相应最高的安全完整性等级。

如果一个单独的 E/E/PE 系统能提供所有要求的安全功能，而且要求的安全完整性等级低于 SIL1，那么 GB/T 20438 不适用。

4.5 功能安全示例回顾

安全功能要求与安全完整性要求组成功能安全要求规范。这些要求必须在设计 E/E/PE 安全相关系统前全部确定。

在第 3 章所述示例中，对该特定危险事情的功能安全要求描述如下：

示例：当防护罩打开 5 mm 或更大开度时，电机应当断电，刹车制动，使叶片在 1 s 内停下，此安全功能的安全完整性等级应为 SIL2。

功能安全要求规范关注安全相关系统作为一个整体在特定环境下的行为。在此例中，E/E/PE 安

全相关系统包括保护联锁开关、电路、接触器、电机和刹车。

4.6 GB/T 20438 框架

GB/T 20438 由以下部分组成：

GB/T 20438.1—2006，电气/电子/可编程电子安全相关系统的功能安全 第 1 部分：一般要求

GB/T 20438.2—2006，电气/电子/可编程电子安全相关系统的功能安全 第 2 部分：电气/电子/可编程电子安全相关系统的要求

GB/T 20438.3—2006，电气/电子/可编程电子安全相关系统的功能安全 第 3 部分：软件要求

GB/T 20438.4—2006，电气/电子/可编程电子安全相关系统的功能安全 第 4 部分：定义和缩略语

GB/T 20438.5—2006，电气/电子/可编程电子安全相关系统的功能安全 第 5 部分：确定安全完整性等级的方法示例

GB/T 20438.6—2006，电气/电子/可编程电子安全相关系统的功能安全 第 6 部分：GB/T 20438.2和 GB/T 20438.3 的应用指南

GB/T 20438.7—2006，电气/电子/可编程电子安全相关系统的功能安全 第 7 部分：技术和措施概述

GB/T 20438 各部分要求框图见图 1。

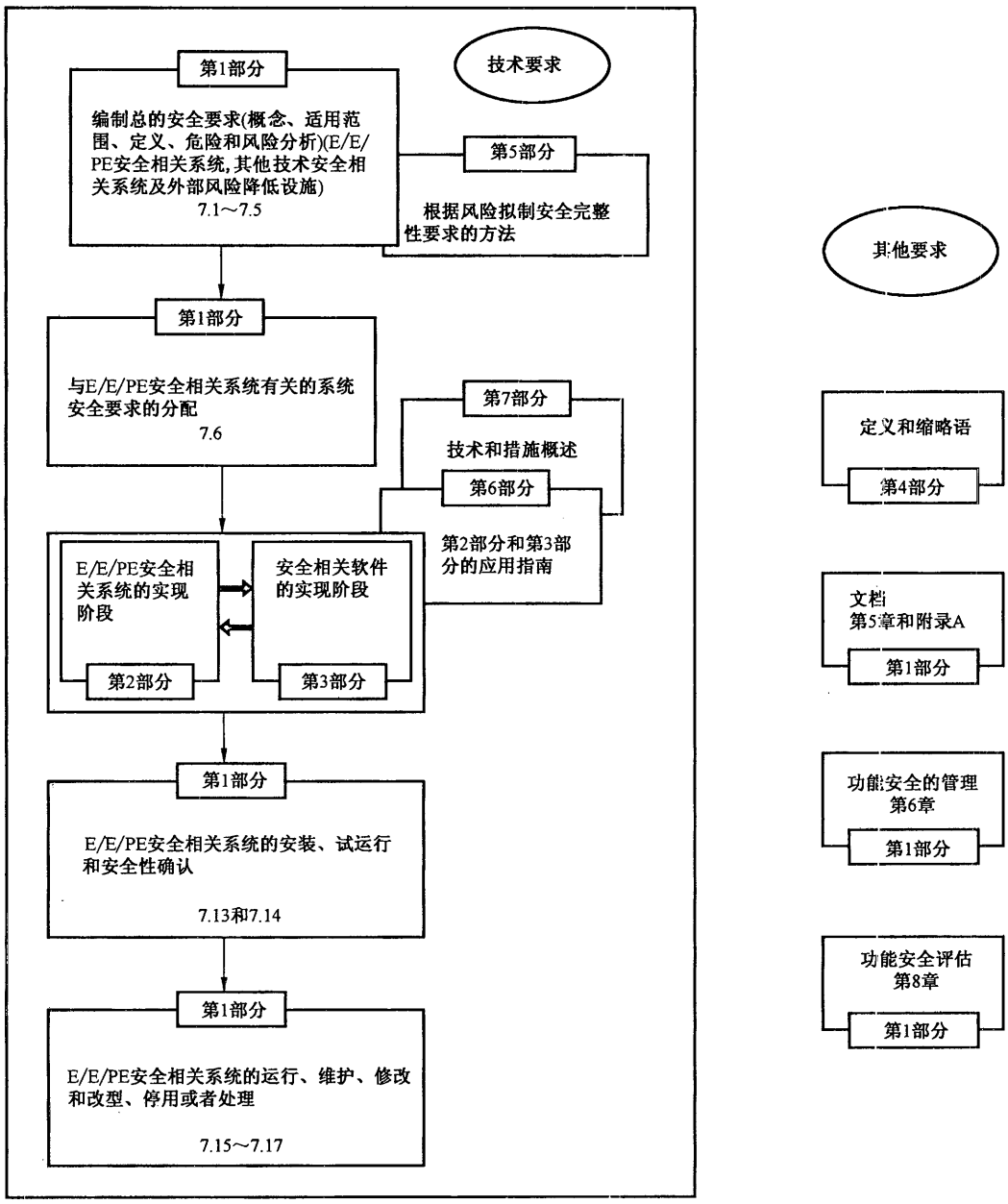

图 1 GB/T 20438 第 1～7 部分的要求的框图

4.7 GB/T 20438 作为其他标准的基础

如果某一技术委员会通过危险分析确定需要有足够的保护以应对重大危险或危险事件,则标准的制定者应在安全标准中考虑功能安全。

GB/T 20438 的第 1～4 部分是基本安全出版物。只要能适用,技术委员会的职责之一就是在其各自的领域标准或产品标准制定中使用 GB/T 20438 的这些部分(当 E/E/PE 安全相关系统在这些标准范围内)。更多的信息可见 GB/T 16499 和 GB/T 20000.4。

GB/T 20438 是各领域(如过程领域)已发布标准的基础,同时也是制定其他领域标准和产品标准的基础。因此,它将影响各领域的 E/E/PE 安全相关系统和产品的开发。

基于 GB/T 20438 的具体领域标准:

——针对系统设计者、系统集成商和用户；
——考虑到具体领域的实际情况，允许简化要求；
——使用行业术语使表达更清晰；
——可规定适用于该领域的特殊限制；
——按照 GB/T 20438 的要求进行子系统的详细设计；
——允许最终用户无需考虑 GB/T 20438 来实现功能安全。

GB/T 20438 作为基本安全出版物不适用于简单的 E/E/PE 安全相关系统(见 GB/T 20438.1 的 4.2)。此类 E/E/PE 安全相关系统中，很好地定义了每个独立元件的失效模式，而且能完全确定在故障状况下的系统行为。例如，包含一个或多个限位开关的系统，该系统操作一个或多个接触器，可能还要通过一些中间继电器来切断电机电源。

4.8 GB/T 20438 作为独立的标准

GB/T 20438 的所有部分可被工业界直接用作独立出版物。它可以如下使用：
——作为 E/E/PE 安全相关系统的一组通用要求，可以使用在没有领域标准和产品标准的地方或领域标准不适用的情况下；
——所有领域的 E/E/PE 部件和子系统的供货商使用(例如传感器的软件和硬件、智能执行器、可编程控制器、数据通信)；
——系统构建者用来满足用户对 E/E/PE 安全相关系统的规范要求；
——用户用来规定执行的安全功能的要求以及这些安全功能的性能要求；
——便于维护 E/E/PE 安全相关系统的“设计的”安全完整性；
——为一致性评估和认证服务提供技术框架；
——作为对安全生命周期活动进行评估的基础。

4.9 更多信息

关于功能安全的更多信息，包括常见问题(见附录 A)，可以在 IEC 网站的“功能安全”专区找到(http://www.iec.ch/functionalsafety)。

如果不熟悉标准内容，建议首先阅读以下内容：
——第 5 部分的附录 A(介绍了风险的概念和安全完整性)；
——第 1 部分的图 2 和表 1(图解说明了整体安全生命周期，并列出各生命周期阶段的目的。生命周期和阶段目的帮助理解第 1 部分第 7 章中要求)；
——第 1 部分的第 6 章和第 8 章(包括关于功能安全管理和评估的要求)；
——第 6 部分的附录 A(概述了第 2 部分和第 3 部分的要求)；
——第 2 部分的图 2 和表 1 以及第 3 部分的图 3 和表 1(帮助理解第 2 部分和第 3 部分的第 7 章)。

GB/T 20438 的特殊要求应当在生命周期的各阶段(适用时)和针对该阶段要求声明的目标中考虑，并在陈述该阶段要求前首先声明其目的。

附 录 A
（资料性附录）
IEC“功能安全”专区的常见问题列表

表 A.1 列出了常见问题，其回答见在 IEC 网站“功能安全”专区（http://www.iec.ch/ functional-safety）。在本列表发布后，网站上可能增加了其他问题问答。

表 A.1 常见问题列表

部 分	常见问题
范围	IEC 61508 与我有关吗？ IEC 61508 涵盖哪些系统？ 请给出实际例子 IEC 61508 如何应用在只有一小部分使用 E/E/PE 技术的安全相关系统中？ IEC 61508 如何应用在功能为避免环境破坏或严重经济损失的系统中？ IEC 61508 由哪几部分组成？ 标准可以免费获得吗，比如从互联网下载？ 我已获得一份标准，我应该如何阅读？
在国际标准框架中的位置	该标准如何在国际范围内发布？ IEC 61508 的国际地位如何？ IEC 61508 如何与各领域标准相配合？ 什么是基本安全出版物？ 基于 IEC 61508 的应用领域或子系统标准有哪些？ IEC 61508 中安全完整性的 1-4 级如何转化成 EN 954-1 中的等级或二者有何联系？ IEC 61508 能否独立使用？ 是否会修订 IEC 61508？ 在修订过程中是否可以提意见？
地区因素和技术解释	如何在 IEC 61508 中找到适合我国的信息？ IEC 61508 也是欧洲标准吗？ 是否按照某些欧盟指令强制使用 IEC 61508？ 如何获得标准特定子条款的技术解释？ 如何与我国的国家委员会联系？
符合标准	需要满足什么条件才能声明符合此标准？ IEC 61508 如何运用在低复杂性的 E/E/PE 安全相关系统中？ E/E/PE 安全相关系统中不同安全功能的安全完整性对应怎样的 IEC 61508 要求？ 是否有必要选用 IEC 61508-2 和 IEC 61508-3 的附录 A 和 B 建议的技术和措施以符合此标准？ 在 E/E/PE 安全相关系统中，我作为部分（不是全部）开发阶段的合同方。为了符合 IEC 61508，在建立文档时，我需要从其他参与方中得到哪些信息？ 供货商提出其产品符合 IEC 61508 的特定安全完整性等级。这是否意味着只要我使用这些产品就符合 IEC 61508？ 我提供将使用在安全相关系统中的子系统，如传感器或执行器。IEC 61508 对我来说意味着什么？

表 A.1（续）

部　分	常见问题
符合标准	为了符合 IEC 61508，是否需要使用经过第三方认证的部件？ 功能安全评估要求的独立性水平与第三方认证的需求之间有何联系？ 如何考虑人员活动对 E/E/PE 安全相关系统运行的影响？ E/E/PE 安全相关系统是否可包含没有按照 IEC 61508 生产的硬件和(或)软件，并仍然符合此标准？ 向安全相关系统发出命令的控制系统是否也被认为是安全相关系统？ 电磁抗扰性限值与安全完整性有怎样的关系？
重要概念	什么是功能安全？ 根据 IEC 61508，什么是安全相关系统？ E/E/PE 是什么意思？ 低复杂性的 E/E/PE 安全相关系统是什么？ 什么是安全完整性等级(SIL)？ 在安全完整性定义为失效率的情况下，软件安全完整性是什么意思？ SIL 系统、子系统或部件是什么意思？ 什么是功能安全评估？ 什么是操作模式？ 低要求操作模式与高要求或连续操作模式有什么不同？ 请给出不同操作模式的结构示例 操作模式是否影响安全完整性的确定？ 什么是受控设备(EUC)
危险与风险分析	IEC 61508 是否仅通过提高可靠性来保证安全？ IEC 61508 是否涵盖危险源的消除？ IEC 61508 是否要求执行定量风险分析来确定安全完整性等级？ 当使用风险图方法确定安全完整性等级时，需要考虑哪些因素？ 应该如何考虑由 E/E/PE 安全相关系统引入的危险？